UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SUNLIFE TOTAL HEALTH INC.

Plaintiff,

-against-

JPMORGAN CHASE BANK, N.A.,

Defendant.

CASE No.

COMPLAINT

Plaintiff Sunlife Total Health Inc. ("Sunlife" or "Plaintiff") alleges for its complaint against Defendant JPMorgan Chase Bank, N.A. ("Chase" or "Defendant"), to the best of its knowledge, information and belief, formed after an inquiry reasonable under the circumstances:

NATURE OF THE ACTION

1. This action arises from the conduct of Chase in its failure to use commonsense and commercially reasonable efforts to verify, authenticate, and prevent six (6) fraudulent and unauthorized wire transfers of funds out of Sunlife's account as required by law and the applicable agreements between the parties. Chase's failures were compounded by the negligence and wrongful conduct of Chase in subsequently refusing to reimburse Sunlife.

2. As a direct result of Chase's wrongful conduct, a total of $198,485 was transferred out of Sunlife's account via Chase's online banking system without authorization (the "Unauthorized Wire Transfers"). To date, none of those funds have been recovered or replaced by Chase. Worse, Chase has instead decided to abandon its accountholder altogether, shamelessly refusing to respond substantively to any of the several inquiries made by Sunlife.

3. As alleged in greater detail below, Defendants' conduct constitutes, *inter alia*, a violation of Federal Reserve Board Regulation J, Subpart B, 12 C.F.R. § 210.25 et seq. ("Regulation J"), a violation of Article 4A of New York's Uniform Commercial Code, negligence,

breach of contract, breach of the covenant of good faith and fair dealing, breach of fiduciary duties, deceptive business practices, fraud, and negligent misrepresentation.

PARTIES

4. Plaintiff Sunlife is a New York corporation with its principal place of business in the Bronx, New York.

5. Defendant Chase is a national banking association with its corporate headquarters in New York, New York.

JURISDICTION AND VENUE

6. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1331, because the dispute arises out of wire transfers subject to Federal Reserve Board Regulation J, Subpart B, 12 C.F.R. § 210.25 et seq. ("Regulation J"). Therefore, the right to relief depends on resolution of a question of federal law.

7. This Court has supplemental jurisdiction over all state law claims pursuant to 28 U.S.C. § 1367.

8. This Court has personal jurisdiction over Chase because it is headquartered in New York and transacted business in New York concerning the acts, transactions and circumstances relating to the claims alleged herein.

9. Venue is proper under 28 U.S.C. § 1391(a) because Chase is subject to personal jurisdiction in this District and/or a substantial part of the events or omissions that give rise to the claims occurred or property that is the subject of the action is situated in this District.

STATEMENT OF FACTS

10. Sunlife is a company that produces herbal wellness products located in the Bronx. Sunlife owns and maintains a business checking ending in 3816 (the "Account") with Chase.

11. At all relevant times, Chase was required to and agreed to follow – and represented that it always followed – a write transfer authentication process. Pursuant to this process, Chase promised it would provide multiple authentication checks and would send temporary identification codes that its accountholders could use to securely sign into their accounts and process wire transactions. If there was any suspicious activity on an account, Chase would contact the accountholder and place a temporary hold on the accountholder's online activity to make sure no one else was attempting to access the account. Chase also promised to use encryption technology to protect an accountholder's username, password, and other personal account information when the accountholder was using its site or apps.

12. Here, however, Chase failed to comply with its own authentication process as well as its legal and contractual obligations, causing Sunlife to fall victim to a devastating fraud resulting in the theft of nearly $200,000 from Sunlife's account.

13. In or about September 2022, an unidentified threat actor successfully conducted a business email compromise attack and gained control of at least one of Sunlife's email accounts. Using the compromised email account, the threat actor hacked into the Chase Account and arranged for a series of wire transfers to be made to the threat actor's own bank accounts located in Dubai, United Arab Emirates.

14. The series of wire transfers occurred over four days on September 21, 2022, September 26, 2022, September 28, 2022, and September 28, 2022, as follows:

Wire Transfer Date	Amount	Beneficiary	Address
9/21/2022	$ 21.00	Kaka Michael	Emirates Mall Dubai
9/26/2022	$ 23.00	Kaka Michael	Emirates Mall Dubai
9/27/2022	$ 49,210.00	Kaka Michael	Emirates Mall Dubai
9/27/2022	$ 49,870.00	Kaka Michael	Emirates Mall Dubai
9/28/2022	$ 49,450.00	Kaka Michael	Emirates Mall Dubai
9/28/2022	$ 49,911.00	Kaka Michael	Emirates Mall Dubai
Total	**$ 198,485.00**		

15. The fraudulent scheme was discovered by Sunlife a few days after the Unauthorized Wire Transfers were completed. However, before the fraudulent scheme was discovered, Chase – without following its own authentication process or obtaining authorization as required – executed the six requested wire transfers. A total of $198,485 was transferred from Sunlife's account to the oversea accounts in Dubai held by the threat actor.

16. The Unauthorized Wire Transfers were extremely uncharacteristic for Sunlife's account. Prior to the Unauthorized Wire Transfers, Sunlife never issued an international wire transfer, let alone one as high as $49,000. Thus, the Unauthorized Wire Transfers were conspicuously unlike the normal activity for Sunlife's account. They should have been flagged as suspicious and triggered further action by Chase.

17. Chase was on actual notice of the risk of this exact type of fraudulent activity.

18. In response to increasing threats of fraud and identity theft, the Federal Financial Institutions Examination Council ("FFIEC") issued guidance titled *Authentication in an Internet Banking Environment* in October 2005 (the "2005 Guidance"). In the 2005 Guidance, the FFIEC set forth recommendations and standards with respect to risk management and customer authentication for financial institutions offering internet-based products and service. The FFIEC concluded that "[f]inancial institutions offering Internet-based products and services should have reliable and secure methods to authenticate their customers."

19. The FFIEC determined that on its own, single-factor authentication is an inadequate form of authentication for "high-risk transactions involving access to customer information or the movement of funds to other parties." It therefore urged financial institutions to conduct risk assessments to evaluate the adequacy of their authentication techniques in light of new or changing risks such as phishing, pharming, malware, and the evolving sophistication of compromise techniques.

20. The FFIEC also endorsed the use of layered security and monitoring systems to detect and prevent fraud and unauthorized access to computer systems and customer accounts. When single-factor authentication is found to be inadequate, financial institutions should implement multifactor authentication.

21. A properly designed and implemented multifactor authentication procedure is a more reliable and stronger fraud deterrent than a security procedure that relies on single-factor authentication.

22. In a "Frequently Asked Questions" publication supplementing the 2005 Guidance, the FFIEC stated, "any system that permits the movement of funds to other parties and/or the access to customer information, as previously defined, is 'high risk' necessitating stronger authentication or additional controls."

23. On June 22, 2011, the FFIEC issued further guidance titled *Supplement to Authentication in an Internet Banking Environment* (the "2011 Guidance"). In the 2011 Guidance, the FFIEC noted that the online threat environment was evolving to become more treacherous, as fraudsters and organized criminal groups continued to develop and deploy more sophisticated, effective, and malicious methods to compromise authentication methods and controls to gain

unauthorized access. The FFIEC was concerned that even customer authentication methods and controls that complied with the 2005 Guidance were now stale and less effective.

24. The 2011 Guidance specifically identified online commercial ACH transactions as posing a greater threat level of risk than online consumer transactions. The FFIEC therefore stated that "[f]inancial institutions should implement layered security, as described herein, utilizing controls consistent with the increased level of risk for covered business transactions." It also reiterated its recommendation that "institutions offer multifactor authentication to their business customers."

25. According to the FFIEC, "[l]ayered security is characterized by the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control." As recommended by the FFIEC, layered security controls should include processes to monitor or detect suspicious activity related to (i) initial login and authentication; and (ii) initiation of electronic transfers of funds.

26. The FFIEC noted that "[t]ransaction monitoring/anomaly detection software has been in use for a number of years" and are available to "monitor online banking activity for suspicious funds transfers." Such software can also "stop a suspicious ACH/wire transfer before completion and alert the institution and/or the customer so that the transfer can be further authenticated or dropped." Out-of-band authentication was also identified as an increasingly popular and effective means of security to prevent unauthorized funds transfers.

27. The 2011 Guidance also identified certain security procedures that have become outdated and ineffective. "Simple device identification" and "basic challenge questions," for example, as primary controls, are no longer considered to be effective risk mitigation techniques.

28. Chase made specific representations about its security and verification procedures to its accountholders, including Sunlife. For example, Chase's website boasts all the ways it "protects" its clients:

- Chase conducts "multiple authentication checks": "When you sign in for the first time or with a device we don't recognize, we'll ask you for your username, password and a temporary identification code, which we'll send you by phone, email or text message. Once you give us the identification code, we'll sign you securely into your accounts. This multistep process helps us protect your accounts and lets us recognize your device the next time you sign in. For extra security, we might ask you to do this again when you enroll in or start using new products (for example, our wire transfer service)."

- Chase monitors "suspicious activity": "We monitor your chase.com profile to help us detect fraud as early as possible. We might call you if we notice a change in your online activity, but we'll never ask you for personal information over the phone, such as your mother's maiden name or Social Security Number. If we can't reach you, we might place a temporary hold on your online activity to make sure it's you and not someone else using your account. If that happens, call us right away using one of numbers on How to Report Fraud to confirm your account activity, and you can start using your online and mobile access again."

- Chase provides state of the art "encryption technology": "We use 128-bit encryption technology to protect your username, password and other personal account information when you're using our site or apps. You'll know your information is encrypted when the chase.com page you're on starts with 'https://' and you see a lock symbol in your web browser."

29. Although Chase should and would have discovered that the wire transfers were unauthorized and fraudulent had it simply followed its own internal procedures, complied with its legal and contractual obligations, or acted consistent with commercially reasonable practices, it failed to do so. Instead, Chase took no action.

30. Upon learning of the fraud and resulting theft, Sunlife immediately notified Chase's forgery department and submitted a Statement of Fact affidavit stating that it did not authorize any of the wire transfers. Chase eventually responded stating that it "made several attempts to recall the funds on [Plaintiff's] behalf but unfortunately they have been unsuccessful. We recommend that you contact the beneficiary and attempt to settle the matter directly."

31. In early November 2022, Sunlife retained counsel to help assist it with reimbursement of the stolen funds. Sunlife's counsel contacted Chase's forgery department on November 15, 2022, November 28, 2022, and December 5, 2022. On each call, various Chase representatives confirmed that no authentication or security alerts concerning the suspicious activity on Sunlife's Account were reported to Sunlife before or after the Unauthorized Wire Transfers were processed.

32. To date, Chase has not offered any substantive response to Sunlife's reimbursement request. Chase completely abdicated all of its responsibilities.

33. As a direct and proximate result of the conduct of Chase as described herein, Sunlife has incurred substantial damages.

FIRST CLAIM FOR RELIEF
(Negligence)

34. Plaintiff repeats and realleges each and every of the foregoing allegations as if restated in full herein.

35. As Sunlife's depository institution, Chase had a duty to use reasonable care to protect Sunlife's online account from unauthorized access and to keep its account information private and secure.

36. Chase had a duty to use reasonable care in monitoring, detecting, and preventing unauthorized account access and to recover all funds lost due to unauthorized wire transfers.

37. Chase had a duty to follow and implement the recommendations and guidance of the FFIEC, including conducting regular risk assessments, employing a commercially reasonable fraudulent transaction detection system, and using multifactor authentication, layered security, transaction monitoring/anomaly detection software, or a combination of such security procedures to protect high risk transactions like international wire transfers.

38. By the acts and omissions described in the preceding paragraphs, Chase and has breached its respective duties of care owed to Sunlife.

39. As a direct and proximate result of the conduct of Chase as described herein, Sunlife has incurred substantial damages.

SECOND CLAIM FOR RELIEF
(Breach of Contract)

40. Plaintiff repeats and realleges each and every of the foregoing allegations above as if restated in full herein.

41. Sunlife and Chase were parties to an agreement.

42. Despite Sunlife performing its obligations pursuant to the agreement, Chase breached its contractual obligations as described above.

43. Chase's actions were knowing, deliberate, and malicious.

44. Under N.Y.U.C.C. Article 4A, Chase may not contract out of its obligation to refund its customers for unauthorized transfers.

45. As agreed upon in the agreement, Chase had a contractual obligation to verify the authenticity of Sunlife's wire transfers using multi-factor authentication and other security measures.

46. Chase breached the agreement by failing to verify the Unauthorized Wire Transfers through multi-factor authentication and other security measures.

47. As a direct and proximate result of the conduct of Chase as described herein, Sunlife has incurred substantial damages.

THIRD CLAIM FOR RELIEF
(Breach of the Covenant of Good Faith and Fair Dealing)

48. Plaintiff repeats and realleges each and every of the foregoing allegations above as if restated in full herein.

49. Every contract entered into carries an implied covenant of good faith and fair dealing in the course of performance.

50. Implied in the agreement between Sunlife and Chase was the obligation that each party would deal fairly and honestly with the other and not force the other to incur any unnecessary expenses.

51. Chase's conduct constitutes a breach of this implied covenant.

52. Chase's conduct was in bad faith and constitutes a breach of the covenant of good faith and fair dealing.

53. Chase's actions were knowing, deliberate, and malicious.

54. As a direct and proximate result of the conduct of Chase as described herein, Sunlife has incurred substantial damages.

FOURTH CLAIM FOR RELIEF
(Breach of the Covenant of Good Faith and Fair Dealing)

55. Plaintiff repeats and realleges each and every of the foregoing allegations above as if restated in full herein.

56. Due to the relative positions of the parties, a fiduciary relationship existed between Chase and Sunlife.

57. Sunlife placed its trust and confidence in Chase to protect its deposits and online bank accounts through a commercially reasonable security procedure.

58. Chase breached its fiduciary duty to Sunlife by failing protect Chase's deposits and online accounts through a commercially reasonable security procedure.

59. As a direct and proximate result of the conduct of Chase as described herein, Sunlife has incurred substantial damages.

FIFTH CLAIM FOR RELIEF
(Deceptive Acts and Practices, N.Y.G.B.L. § 349)

60. Plaintiff repeats and realleges each and every of the foregoing allegations above as if restated herein.

61. Chase's conduct as described herein was consumer-oriented and materially misleading.

62. As a direct and proximate result of the conduct of Chase as described herein, Sunlife has incurred substantial damages.

SIXTH CLAIM FOR RELIEF
(Fraud)

63. Plaintiff repeats and realleges each and every of the foregoing allegations above as if restated herein.

64. Chase made representations to Sunlife that it used multifactor authentication and a commercially reasonable fraudulent transaction detection system to secure its online bank accounts.

65. Chase intended for Sunlife to rely on those representations.

66. At the time these representations were made, Chase knew that it did not use multifactor authentication or a commercially reasonable fraudulent transaction detection system to secure Sunlife's online bank accounts.

67. The strength of Chase's fraud prevention controls and security procedures were material factors in Sunlife's decision to create online accounts with Chase.

68. Sunlife reasonably relied on Chase's representations regarding the strength of its fraud prevention controls and security procedures.

69. As a direct and proximate result of the conduct of Chase as described herein, Sunlife has incurred substantial damages.

SEVENTH CLAIM FOR RELIEF
(Negligent Misrepresentation)

70. Plaintiff repeats and realleges each and every of the foregoing allegations above as if restated in full herein.

71. At all times, Sunlife has been concerned about the security of its bank accounts and banking transactions.

72. Chase negligently represented to Sunlife that its account would be protected through a commercially reasonable security procedure, including the use of multifactor authentication.

73. In fact, Sunlife's account was not protected through a commercially reasonable security procedure and was not secured using multifactor authentication.

74. Sunlife foreseeably and reasonably relied upon Chase's misrepresentations.

75. As a direct and proximate consequence of Sunlife's justifiable reliance on Chase's misrepresentations, Sunlife lost hundreds of thousands of dollars in unauthorized wire transfers.

76. As a direct and proximate result of the conduct of Chase as described herein, Sunlife has incurred substantial damages.

EIGHTH CLAIM FOR RELIEF
(Failure to Verify Funds Transfer, N.Y. U.C.C. §§ 4A-202, 4A-203)

77. Plaintiff repeats and realleges each and every of the foregoing allegations above as if restated in full herein.

78. Wire transactions from accounts held at Chase are governed by Article 4A of the Uniform Commercial Code, codified at N.Y.U.C.C. § 4A-101, et seq.

79. Chase never offered Sunlife a commercially reasonable security procedure to protect wire transfers initiated through its Account.

80. Chase did not verify the Unauthorized Wire Transfers through a security procedure that was commercially reasonable.

81. Sunlife never refused a security procedure offered by Chase that was commercially reasonable. Accordingly, Sunlife never agreed to be bound by a security procedure that Sunlife itself selected, which was different than a security procedure that Chase offered.

82. Sunlife promptly notified Chase of the Unauthorized Wire Transfers as soon as it was alerted of the fraudulent wire transfers.

83. The Unauthorized Wire Transfers were not authorized by Sunlife or any of its employees, officials, agents, or representatives.

84. Even though the Unauthorized Wire Transfers deviated from Sunlife's typical bank transactions and had characteristics that were anomalous, Chase still accepted and processed them.

85. Chase did not accept the Unauthorized Wire Transfers pursuant to a commercially reasonable security procedure and did not accept the payment orders in good faith, in violation of N.Y.U.C.C. § 12A:4A-202.

86. As a direct and proximate result of the conduct of Chase as described herein, Sunlife has incurred substantial damages.

87. Under N.Y.U.C.C. § 4A-204, Chase must therefore refund the full amount of the unauthorized payments plus interest, calculated from the date of the Unauthorized Wire Transfers.

NINTH CLAIM FOR RELIEF
(Violation of Regulation J)

88. Plaintiff repeats and realleges each and every of the foregoing allegations above as if restated in full herein.

89. Funds transferred through the Federal Reserve Wire Transfer Network ("Fedwire") are governed by Regulation J, which incorporates Article 4A of the Uniform Commercial Code.

90. Regulation J requires a bank to adopt a commercially reasonable method of providing security against unauthorized payment orders. In order to be "commercially reasonable," the security procedure is required to take into account, *inter alia*, the "size, type and frequency of payment orders normally issued by the customer to the bank." *Id*. (incorporating U.C.C., § 4A-202(c)).

91. Regulation J, adopting U.C.C §4A-204, also requires that "[i]f a receiving bank accepts a payment order issued in the name of its customer as sender which is ... not authorized and not effective as the order of the customer ... the bank shall refund any payment of the payment order received from the customer to the extent the bank is not entitled to enforce payment and shall pay interest on the refundable amount calculated from the date the bank received payment to the date of the refund."

92. Regulation J further provides that in order to be eligible to receive interest on the refundable amount, the customer must inform the bank of the unauthorized wire transfer within "a reasonable time." The statute defines a "reasonable time" as "not exceeding 90 days after the date the customer received notification from the bank that the order was accepted or that the customer's account was debited with respect to the order."

93. Upon information and belief, the Unauthorized Wire Transfers were made through Fedwire. Because the Unauthorized Wire Transfers were made through Fedwire, they are subject to Regulation J.

94. By wiring funds from the Account without Sunlife's authorization, despite the fact that the Unauthorized Wire Transfers were an aberration from the Account's usual banking activity, Chase failed to adhere to commercially reasonable security procedures, in violation of Regulation J.

95. Pursuant to Regulation J, Chase must therefore refund the full amount of the unauthorized payments plus interest, calculated from the date of the Unauthorized Wire Transfers.

DEMAND FOR A JURY TRIAL

Pursuant to Fed. R. Civ. P. 38, Plaintiff hereby demands a jury trial of all issues capable of being determined by a jury.

WHEREFORE, Plaintiff requests judgment against Defendant as follows:

i. Awarding damages against Defendant in favor of Plaintiff in an amount to be determined at trial;

ii. attorney's fees, disbursements, and costs of the action; and,

iii. and other such other relief as the Court deems just and proper.

Dated: New York, New York
December 28, 2022

GOLDENBERG LAW, P.C.

By: */s/ Andrew R. Goldenberg*
Andrew R. Goldenberg
11 Broadway, Suite 615
New York, New York 10004
Telephone: (212) 906-4499

Attorneys for Plaintiff Sunlife Total Health Inc.